

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

In the Matter of a Warrant for All
Content and Other Information
Associated with the iCloud Accounts
[REDACTED]@gmail.com and
[REDACTED]@icloud.com
Maintained at Premises Controlled by
Apple Inc., USAO Reference No.
2021R00778

TO BE FILED UNDER SEAL

AGENT AFFIDAVIT

22 MAG 6274

**Agent Affidavit in Support of Application for a Search Warrant
for Stored Electronic Communications**

STATE OF NEW YORK)
) ss.
COUNTY OF NEW YORK)

[REDACTED], being duly sworn, deposes and states:

I. Introduction

A. Affiant

1. I have been a Special Agent with the Federal Bureau of Investigation ("FBI") for over two years. I am assigned to a public corruption squad in the FBI's New York office and have participated in investigations involving campaign finance offenses and public corruption. As part of those investigations, I have participated in the execution of search warrants involving electronic evidence.

B. The Provider, the Subject Accounts and the Subject Offenses

2. I make this affidavit in support of an application for a search warrant pursuant to 18 U.S.C. § 2703 for all content and other information associated with the iCloud accounts [REDACTED]@gmail.com (the "[REDACTED] Account") and [REDACTED]@icloud.com (the "[REDACTED] Account") (together the [REDACTED] Account and the [REDACTED] Account are the "Subject

Accounts”), maintained and controlled by Apple Inc. (the “Provider”), headquartered at 1 Infinite Loop, Cupertino, California 95014. The information to be searched is described in the following paragraphs and in Attachment A to the proposed warrant.

3. As detailed below, there is probable cause to believe that the Subject Accounts contain evidence, fruits, and instrumentalities of violations of theft of federal funds and wire fraud, and conspiracy to commit the same, in violation of 18 U.S.C. §§ 371, 666, 1343, and 1349 (the “Subject Offenses”). This affidavit is based upon my personal knowledge, my review of documents and other evidence, and my conversations with other law enforcement officers, as well as my training and experience concerning the use of email in criminal activity. Because this affidavit is being submitted for the limited purpose of establishing probable cause, it does not include all the facts I have learned during my investigation. Where the contents of documents and the actions, statements, and conversations of others are reported herein, they are reported in substance and in part, except where otherwise indicated.

C. Services and Records of the Provider

4. I have learned the following about the Provider:

a. Apple is a United States company that produces the iPhone, iPad, and iPod Touch, all of which use the iOS operating system, and desktop and laptop computers based on the Mac OS operating system.

b. Apple provides a variety of services that can be accessed from Apple devices or, in some cases, other devices via web browsers or mobile and desktop applications (“apps”). As described in further detail below, the services include email, instant messaging, and file storage:

i. Apple provides email service to its users through email addresses at the domain names mac.com, me.com, and icloud.com.

ii. iMessage and FaceTime allow users of Apple devices to communicate in real-time. iMessage enables users of Apple devices to exchange instant messages (“iMessages”) containing text, photos, videos, locations, and contacts, while FaceTime enables those users to conduct audio and video calls.

iii. iCloud is a cloud storage and cloud computing service from Apple that allows its users to interact with Apple’s servers to utilize iCloud-connected services to create, store, access, share, and synchronize data on Apple devices or via icloud.com on any Internet-connected device. For example, iCloud Mail enables a user to access Apple-provided email accounts on multiple Apple devices and on iCloud.com. iCloud Photo Library and My Photo Stream can be used to store and manage images and videos taken from Apple devices, and iCloud Photo Sharing allows the user to share those images and videos with other Apple subscribers. iCloud Drive can be used to store presentations, spreadsheets, and other documents. iCloud Tabs and bookmarks enable iCloud to be used to synchronize bookmarks and webpages opened in the Safari web browsers on all of the user’s Apple devices. iCloud Backup allows users to create a backup of their device data. iWork Apps, a suite of productivity apps (Pages, Numbers, Keynote, and Notes), enables iCloud to be used to create, store, and share documents, spreadsheets, and presentations. iCloud Keychain enables a user to keep website username and passwords, credit card information, and Wi-Fi network information synchronized across multiple Apple devices.

iv. Game Center, Apple’s social gaming network, allows users of Apple devices to play and share games with each other.

v. Find My iPhone allows owners of Apple devices to remotely identify and track the location of, display a message on, and wipe the contents of those devices. Find My Friends allows owners of Apple devices to share locations.

vi. Location Services allows apps and websites to use information from cellular, Wi-Fi, Global Positioning System (“GPS”) networks, and Bluetooth, to determine a user’s approximate location.

vii. App Store and iTunes Store are used to purchase and download digital content. iOS apps can be purchased and downloaded through App Store on iOS devices, or through iTunes Store on desktop and laptop computers running either Microsoft Windows or Mac OS. Additional digital content, including music, movies, and television shows, can be purchased through iTunes Store on iOS devices and on desktop and laptop computers running either Microsoft Windows or Mac OS.

c. Apple services are accessed through the use of an “Apple ID,” an account created during the setup of an Apple device or through the iTunes or iCloud services. The account identifier for an Apple ID is an email address, provided by the user. Users can submit an Apple-provided email address (often ending in @icloud.com, @me.com, or @mac.com) or an email address associated with a third-party email provider (such as Gmail, Yahoo, or Hotmail). The Apple ID can be used to access most Apple services (including iCloud, iMessage, and FaceTime) only after the user accesses and responds to a “verification email” sent by Apple to that “primary” email address. Additional email addresses (“alternate,” “rescue,” and “notification” email addresses) can also be associated with an Apple ID by the user. A single Apple ID can be linked to multiple Apple services and devices, serving as a central authentication and syncing mechanism.

d. Apple captures information associated with the creation and use of an Apple ID. During the creation of an Apple ID, the user must provide basic personal information including the user’s full name, physical address, and telephone numbers. The user may also provide means of payment for products offered by Apple. The subscriber information and password associated

with an Apple ID can be changed by the user through the “My Apple ID” and “iForgot” pages on Apple’s website. In addition, Apple captures the date on which the account was created, the length of service, records of log-in times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to and utilize the account, the Internet Protocol address (“IP address”) used to register and access the account, and other log files that reflect usage of the account.

e. Additional information is captured by Apple in connection with the use of an Apple ID to access certain services. For example, Apple maintains connection logs with IP addresses that reflect a user’s sign-on activity for Apple services such as iTunes Store and App Store, iCloud, Game Center, and the My Apple ID and iForgot pages on Apple’s website. Apple also maintains records reflecting a user’s app purchases from App Store and iTunes Store, “call invitation logs” for FaceTime calls, “query logs” for iMessage, and “mail logs” for activity over an Apple-provided email account. Records relating to the use of the Find My iPhone service, including connection logs and requests to remotely lock or erase a device, are also maintained by Apple.

f. Apple also maintains information about the devices associated with an Apple ID. When a user activates or upgrades an iOS device, Apple captures and retains the user’s IP address and identifiers such as the Integrated Circuit Card ID number (“ICCID”), which is the serial number of the device’s SIM card. Similarly, the telephone number of a user’s iPhone is linked to an Apple ID when the user signs into FaceTime or iMessage. Apple also may maintain records of other device identifiers, including the Media Access Control address (“MAC address”), the unique device identifier (“UDID”), and the serial number. In addition, information about a user’s computer is captured when iTunes is used on that computer to play content associated with

an Apple ID, and information about a user's web browser may be captured when used to access services through icloud.com and apple.com. Apple also retains records related to communications between users and Apple customer service, including communications regarding a particular Apple device or service, and the repair history for a device.

g. Apple provides users with five gigabytes of free electronic space on iCloud, and users can purchase additional storage space. That storage space, located on servers controlled by Apple, may contain data associated with the use of iCloud-connected services, including: email (iCloud Mail); images and videos (iCloud Photo Library, My Photo Stream, and iCloud Photo Sharing); documents, spreadsheets, presentations, and other files (iWork and iCloud Drive); and web browser settings and Wi-Fi network information (iCloud Tabs and iCloud Keychain). iCloud can also be used to store iOS device backups, which can contain a user's photos and videos, iMessages, Short Message Service ("SMS") and Multimedia Messaging Service ("MMS") messages, voicemail messages, call history, contacts, calendar events, reminders, notes, app data and settings, Apple Watch backups, and other data. Records and data associated with third-party apps may also be stored on iCloud; for example, the iOS app for WhatsApp, an instant messaging service, can be configured to regularly back up a user's instant messages on iCloud Drive. Some of this data is stored on Apple's servers in an encrypted form but can nonetheless be decrypted by Apple.

D. Jurisdiction and Authority to Issue Warrant

5. Pursuant to 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A), the Government may require a provider of an electronic communications service or a remote computing service, such as the Provider, to disclose all stored content and all non-content records or other information pertaining to a subscriber, by obtaining a warrant issued using the procedures described in the Federal Rules of Criminal Procedure.

6. A search warrant under § 2703 may be issued by “any district court of the United States (including a magistrate judge of such a court)” that “has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

7. When the Government obtains records under § 2703 pursuant to a search warrant, the Government is not required to notify the subscriber of the existence of the warrant. 18 U.S.C. § 2703(a), (b)(1)(A), (c)(2) & (3). Additionally, the Government may obtain an order precluding the Provider from notifying the subscriber or any other person of the warrant, for such period as the Court deems appropriate, where there is reason to believe that such notification will seriously jeopardize an investigation. 18 U.S.C. § 2705(b).

II. Probable Cause

A. Probable Cause Regarding the Subject Offenses

8. Since in or about August 2021, the FBI and the Office of the United States Attorney for the Southern District of New York have been investigating the possible receipt of so-called “straw” donations by the 2021 New York City mayoral campaign of Eric Adams (the “Adams Campaign”) from employees of [REDACTED] a construction company that operates in New York City. A straw, or “conduit,” donation occurs when a donation to a political campaign is made in the name of one donor, but the funds in question in fact belong to a different person. This warrant seeks permission to search iCloud accounts used by [REDACTED] and [REDACTED], two individuals associated with Adams who have acted as points of contact between the Adams Campaign and [REDACTED].

The Adams Campaign and New York City’s Matching Funds Program

9. I understand, based on my review of publicly available information, that:

a. The Adams Campaign accepted matching funds from the New York City Campaign Finance Board throughout a significant part of its campaign (“Matching Funds”),

meaning that the Adams Campaign received funds from the New York City government as a result of donations the Adams Campaign received from private donors that were eligible for matching funds.¹

b. Under New York City law, the Adams Campaign was eligible to receive \$2,000 in Matching Funds, and no more than \$2,000 in Matching Funds, for each donation of \$250 from an individual donor who resides within New York City. If an individual donated more than \$250, any amount in excess of \$250 would not be eligible for matching funds.²

c. New York City receives in excess of \$10,000 per year in federal funding.³

The Suspected Straw Donations

10. I understand, based on contribution forms provided by the New York City Campaign Finance Board, that the Adams Campaign received the following donations, among others, on May 7, 2021:

AMOUNT	NAME	CITY	STATE	OCCUPATION	EMPLOYER NAME
\$1,500	Arkan, Erden	New York	NY	Owner	[REDACTED]
\$1,200	[REDACTED]	Flushing	NY	Sr. Manager Prod.	[REDACTED]
\$1,250	[REDACTED]	Brooklyn	NY	Account Manager	[REDACTED]

¹ See, e.g., <https://www.nyl.com/nyc/all-boroughs/news/2021/10/08/eric-adams-is-taking-a-rare-step--turning-down-campaign-cash> (reporting on the Adams Campaign's prior acceptance of matching funds and decision to turn down some matching funds as of October 7, 2021); https://www.nycfb.info/VSAppls/CandidateSummary.aspx?as_cand_id=1545&as_election_cycle=2021&cand_name=Adams%2C+Eric+L&office=Mayor&report=summ (New York City Campaign Finance Board's report detailing total public funds disbursed to Adams Campaign).

² See <https://www.nycfb.info/program/how-it-works>.

³ See https://comptroller.nyc.gov/wp-content/uploads/2016/11/Federal_Budget_Vulnerabilities_Memo.pdf

\$1,250	██████████	Flushing	NY	Construction	██████████
\$1,250	██████████	Cliffside Park	NJ	Business Logistics	██████████
\$1,250	██████████	Brooklyn	NY	PM	██████████
\$1,250	██████████	Brooklyn	NY	Engineer/Lawyer	██████████
\$1,250	██████████	Brooklyn	NY	Project manager	██████████
\$1,250	██████████	Ridgewood	NJ	Finance Director	██████████
\$1,250	██████████	Flushing	NY	Partner	██████████
\$1,250	██████████	New York	NY	Accountant	██████████

The individuals listed in this table are hereinafter referred to as the "Donors."

11. I have further confirmed that, with the exception of the donations by ██████████ and ██████████, Matching Funds were issued in connection with each of the donations identified above.⁵

12. Bank records for ██████████ indicate that on April 28, 2021, ██████████ issued checks in the amount of \$1,250 to each of the Donors with the exception of Arkan and ██████████, and also issued a \$1,250 check to ██████████. I know from law enforcement databases that ██████████ is ██████████ spouse. I know from my review of emails sent to and from each of the Donors except for ██████████,

⁴ The description of ██████████ as an "Engineer/lawyer" at ██████████ is taken from the donation form submitted to the New York City Campaign Finance Board as part of her donation, but it appears from publicly available information that ██████████ may not in fact be employed at ██████████, although as explained in ¶ 12, her husband does appear to be employed at ██████████.

⁵ I understand that Matching Funds are only available for donations made by persons who reside in New York City, and both ██████████ and ██████████ reside in New Jersey.

and also including emails sent to and from [REDACTED] (collectively, the "[REDACTED] Emails"), obtained pursuant to a search warrant, that [REDACTED] is also employed by [REDACTED]. As noted above, Arkan's donation to the Adams Campaign identifies Arkan as an or the owner of [REDACTED]. Thus, on April 28, 2021, [REDACTED] paid each of the Donors the amount of their May 7, 2021 donation, with the exceptions of [REDACTED], whose husband instead received a check for that amount; Arkan, whose donation form describes him as the owner of [REDACTED]; and [REDACTED] who donated \$50 less to the Adams Campaign than [REDACTED] received from [REDACTED].

The [REDACTED] Emails

13. I know from my review of the [REDACTED] emails, in substance and in part, that:

a. On April 10, 2021, Arkan sent an email (the "April 10 Email") in Turkish^{6, 7} to seven individuals, five of whom have corporate email addresses indicating involvement in the construction industry. Arkan also copied seven [REDACTED] employees, of whom four are Donors and one of whom, [REDACTED], is the husband of a Donor. Arkan wrote, in substance and in part, that: In the previous week he had met with (then) Brooklyn Borough President Eric Adams, and the New York General Consul (who I understand, based on information discussed below, to be Turkey's New York General Consul) also joined them; Adams is running for New York City Mayor and has warm feelings for Turkish business people; Arkan knows that the recipients of the email have been supporting Adams so far, but "they" (from context, [REDACTED]) are organizing a very special event in Arkan's office on May 5th, between 5 and 6:30 pm; the recipients of the email should participate in the event and contribute; this may "feel like swimming against the current" but unfortunately,

⁶ Many of the [REDACTED] emails are written wholly or partly in Turkish. I have reviewed draft summaries of those emails prepared by a Turkish linguist employed by the FBI, which are reflected in this Affidavit. Quotations to these emails are to the summaries prepared by the linguist.

⁷ Based on my review of publicly available information, [REDACTED] is affiliated with a larger Turkish company and many of its employees are Turkish nationals.

this is how things are done in this country; and this will hopefully be a successful fundraising event.

b. On April 21, 2021, Arkan sent an email to four individuals to thank them all for participating in an unspecified event. Arkan further wrote that in the morning, he had spoken with “Consul General [REDACTED],” who was very happy and thought that mid-May would be an appropriate target date. I know from publicly available materials that [REDACTED] is the consul general of Turkey’s New York consulate.

c. On April 26, 2021, [REDACTED] (a Donor and [REDACTED] employee) asked Arkan: “Do you want me to email all the people on our list that are capable of making contributions to find out if they are willing to do it? Also Food and beverages, who would you like me to get to cater it?” Arkan responded by forwarding [REDACTED] the April 10 Email.

d. From on or about April 27, 2021 through on or about May 7, 2021, [REDACTED] sent a series of emails inviting persons and businesses associated with [REDACTED], including the recipients of the April 10 Email, to attend a fundraiser for the Adams Campaign, which Adams personally was scheduled to attend, hosted by [REDACTED] on May 7, 2021. Arkan and [REDACTED] were consistently copied on these emails.

e. On April 27 and 28, 2021, Arkan exchanged three emails with [REDACTED], who is not a Donor but, based on his email address and the statements in his email, is a [REDACTED] employee. In the first email, [REDACTED] responds to one of the emails sent by [REDACTED] described above in paragraph 13(d), asking whether he should set up a “‘go fund me’ kind of thing and share the link with everyone” so that the group could raise funds for Adams toward a target amount using a website. Arkan replied in Turkish and only to [REDACTED], stating that it would “cramp their style” to use the method proposed by [REDACTED]. Arkan further explained that “the goal is to host the man

there and to hand the checks to his secretary,” that [REDACTED] method “is too professional” and that [REDACTED] “need[s] to be hands on.” [REDACTED] replied that he would “polish his checkbook” and attend. According to other [REDACTED] Emails I have reviewed, [REDACTED] donated \$200 to the Adams Campaign.

f. On May 5, 2021, Arkan emailed [REDACTED] and [REDACTED] (another Donor and [REDACTED] employee): “Don’t forget to remind our guest for fundraising event!” Subsequently on May 5, 2021, [REDACTED] sent a “friendly reminder regarding our fundraiser with ‘Eric Adams for Mayor’” to the parties described above in paragraphs 13(a) and 13(d).

g. On May 7, 2021, shortly after the scheduled time for the fundraiser, Arkan thanked [REDACTED], [REDACTED], and [REDACTED] (another Donor and [REDACTED] employee) for their hard work in making “this event” successful. Arkan copied [REDACTED] on this email. As noted above, also on May 7, 2021, the Donors made donations to the Adams Campaign that largely matched the amount of money [REDACTED] had paid them on April 28, 2021.

14. On May 10, 2021, [REDACTED] sent [REDACTED] an email with no subject heading or body, attaching a photograph of a handwritten list (the “List”). The List is entitled “Eric Adams 2021 Donation,” and consists of a column of names with corresponding dollar amounts. The List includes all of the Donors and accurately reflects the amount of their donations, except that [REDACTED] is listed as a donor of \$1,250, when according to records maintained by the New York City Board of Elections, it was [REDACTED] wife, [REDACTED]⁸ who donated that amount. The List also reflects smaller donations by ten other individuals or corporations, most of whom appear to have received the emails from [REDACTED] and Arkan urging contribution that are described above in paragraphs 13(a) and 13(d). In total, the list records \$20,000 in donations, of which nearly 70% came from the Donors.

⁸ On the records provided by the New York City Campaign Finance Board, [REDACTED] first name is spelled [REDACTED]. On [REDACTED] bank records as well as the underlying donation slip, however, she uses the common spelling [REDACTED].

B. Probable Cause Regarding the Subject Accounts***The [REDACTED] Account***

15. I know from my review of media reports, among other sources, that [REDACTED] is a longtime advisor of Eric Adams who worked in the Special Counsel's office of the Brooklyn Borough President when Adams was Brooklyn Borough President, was involved with the Adams Campaign, and now works in the Mayor's Office for International Affairs. As detailed below, during the course of Adams's mayoral campaign, [REDACTED] had regular contact both with Turkish consular officials and with [REDACTED] and was personally involved with the May 7, 2021 Adams fundraiser held by [REDACTED], pursuant to which the Donors made their straw donations.

16. Phone records indicate that from between February 8, 2021 and January 14, 2022, a phone number subscribed in [REDACTED] name (the "[REDACTED] Number") exchanged 22 calls with a phone number subscribed to the Turkish Consulate General (the "Consulate Number").⁹ This includes a call on April 2, 2021. As explained above, in the April 10 Email, Arkan stated that he had met with the Consul General and Adams in the prior week, and planned to hold a fundraiser for Adams.

17. Records provided by WhatsApp, an internet-based messaging program, show that between December 3, 2021—which is the first date for which the FBI was able to obtain this data—and August 1, 2022—which is the last date on which I reviewed this data—there were 320 direct WhatsApp communications between an account subscribed to the [REDACTED] number and an account subscribed to the Consulate Number.¹⁰

⁹ These records are not complete, but rather do not include April 2022 and parts of March and May 2022.

¹⁰ These records are not complete, but rather do not include parts of March and April 2022.

18. I have reviewed photographs posted to the Internet on November 18, 2021 by the Turkish General Consulate in New York City showing persons I believe to be [REDACTED], [REDACTED] (the Consul General), and Eric Adams together.

19. Toll records indicate that on May 19, 2021, a phone number subscribed to by [REDACTED] and a phone number subscribed to by Arkan exchanged two calls, one of which resulted in a call of one minute and 11 seconds duration and the other of which did not result in a listed duration (possibly indicating that the call was not answered).

20. On May 20, 2021, Arkan emailed [REDACTED] that [REDACTED] "had called seeking copies of invoices "for the cheese plate and fruits, except the alcohol." Ok then emailed a Gmail account used by [REDACTED] (the "[REDACTED] Gmail") two receipts for purchases of fruits, nuts, juices, and other snack-type items. I understand that campaigns, such as the Adams Campaign, often request receipts of this type because the provision of food and beverages at a campaign event can be considered an "in kind contribution" that campaigns must report, although according to records maintained by New York City Campaign Finance Board, no in-kind donation was reported for this event.

21. On November 2, 2021, Arkan received an email from the [REDACTED] Gmail forwarding information about an Adams campaign election night party and providing an internet link for a "VIP RSVP."

22. I have reviewed records provided by the Provider showing that the [REDACTED] Account is registered using [REDACTED] phone number and address, in addition to using her name as part of the account name. I have consulted with a forensic examiner with the FBI's Computer Analysis Response Team about these records, and I understand that based on the settings on the [REDACTED] Account, the [REDACTED] Account is likely to contain copies of messages sent to or by [REDACTED]

using certain applications such as iMessage (which is often used to send text messages from the Provider's devices) and various email programs, to the extent [REDACTED] used those methods of communication, as well as photographs (such as the one described above in paragraph 18), and calendar, contact, and location information reflecting meetings and other associations. I therefore believe that there is probable cause to believe that evidence of [REDACTED] communications and contacts with [REDACTED] employees and personnel associated with the Turkish General Consulate in New York City, including the Donors and those involved in the suspected straw donations, are likely to be found in the [REDACTED] Account.

The [REDACTED] Account

23. From my review of publicly available information, I know that [REDACTED] was a fundraiser for the Adams Campaign, was employed with the Brooklyn Borough President's office when Adams was the Brooklyn Borough President, and is now a fundraiser for the Kings County Democratic Party. As detailed below, during the period surrounding the coordination of the apparent straw donations, [REDACTED] was in regular contact with [REDACTED] and [REDACTED] (who as discussed above was a [REDACTED] employee coordinating [REDACTED]'s involvement in fundraising for the Adams Campaign), and also received a call from Turkey's Consul General in New York on May 11, 2021.

24. On April 21, 2021, Arkan emailed [REDACTED] the phone number for "[REDACTED] Brooklyn Borough."

25. On April 26, 2021, [REDACTED] emailed Arkan and stated that she had "texted" with [REDACTED], and that [REDACTED] "said the checks can [b]e made payable to: Eric Adams 2021."

26. I have reviewed phone records showing that between April 21, 2021 and May 11, 2021, a phone number used by [REDACTED] communicated with [REDACTED] on approximately 33 occasions,

including by text messages and voice calls. [REDACTED] phone records also show that she communicated twice with a phone number used by [REDACTED] (the Consul General for Turkey in New York) on May 11, 2021. Those records further reflect that between April 2, 2021 and May 5, 2021, [REDACTED] communicated on 32 occasions with a phone number used by [REDACTED]

27. I have reviewed records provided by the Provider showing that the [REDACTED] Account is registered using [REDACTED] phone number, in addition to using her name as part of the account name. I have consulted with a forensic examiner with the FBI's Computer Analysis Response Team about these records, and I understand that based on the settings on the [REDACTED] Account, the [REDACTED] Account is likely to contain copies of messages sent to or by [REDACTED] using applications such as WhatsApp, iMessage (which is often used to send text messages from the Provider's phones) and various email programs, to the extent [REDACTED] used those methods of communication, as well as photographs (such as the one described above in paragraph 18), and calendar, contact, and location information reflecting meetings and other associations. I therefore believe that there is probable cause to believe that evidence of [REDACTED] communications and contacts with [REDACTED] employees and personnel associated with the Turkish General Consulate in New York City, including the Donors and those involved in the suspected straw donations, are likely to be found in the [REDACTED] Account.

28. Temporal Limitation. This application is limited to all content created, sent, or received on or after February 1, 2021 through November 2, 2021, which runs from the earliest month in which the available evidence establishes communications between [REDACTED] and the Turkish General Consulate, and the close of the 2021 election in which the Adams Campaign participated.

C. Evidence, Fruits and Instrumentalities

29. Based upon the foregoing, I respectfully submit there is probable cause to believe that information stored on the Provider's servers associated with the Subject Accounts will contain

evidence, fruits, and instrumentalities of the Subject Offenses, as more fully described in Section II of Attachment A to the proposed warrant.

III. Review of the Information Obtained Pursuant to the Warrant

30. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for service of a search warrant issued under § 2703, or for the collection or production of responsive records. Accordingly, the warrant requested herein will be transmitted to the Provider, which shall be directed to produce a digital copy of any responsive records to law enforcement personnel within 30 days from the date of service. Law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) will retain the records and review them for evidence, fruits, and instrumentalities of the Subject Offenses as specified in Section III of Attachment A to the proposed warrant.

31. In conducting this review, law enforcement personnel may use various methods to locate evidence, fruits, and instrumentalities of the Subject Offenses, including but not limited to undertaking a cursory inspection of all emails within the Subject Accounts. This method is analogous to cursorily inspecting all the files in a file cabinet in an office to determine which paper evidence is subject to seizure. Although law enforcement personnel may use other methods as well, particularly including keyword searches, I know that keyword searches and similar methods are typically inadequate to detect all information subject to seizure. As an initial matter, keyword searches work only for text data, yet many types of files commonly associated with emails, including attachments such as scanned documents, pictures, and videos, do not store data as searchable text. Moreover, even as to text data, keyword searches cannot be relied upon to capture all relevant communications in an account, as it is impossible to know in advance all of the unique

words or phrases that investigative subjects will use in their communications, and consequently there are often many communications in an account that are relevant to an investigation but that do not contain any keywords that an agent is likely to search for.

IV. Request for Non-Disclosure and Sealing Order

32. The existence and scope of this ongoing criminal investigation is not publicly known. As a result, premature public disclosure of this affidavit or the requested warrant could alert potential criminal targets that they are under investigation, causing them to destroy evidence, flee from prosecution, or otherwise seriously jeopardize the investigation. As is set forth above, subjects of this investigation are known to use computers and electronic communications in furtherance of their activity and thus could easily delete, encrypt, or otherwise conceal such digital evidence from law enforcement were they to learn of the Government's investigation. *See* 18 U.S.C. § 2705(b)(3).

33. Accordingly, there is reason to believe that, were the Provider to notify the subscribers or others of the existence of the warrant, the investigation would be seriously jeopardized. Pursuant to 18 U.S.C. § 2705(b), I therefore respectfully request that the Court direct the Provider not to notify any person of the existence of the warrant for a period of one year from issuance, subject to extension upon application to the Court, if necessary.

34. For similar reasons, I respectfully request that this affidavit and all papers submitted herewith be maintained under seal until the Court orders otherwise, except that the Government be permitted without further order of this Court to provide copies of the warrant and affidavit as need be to personnel assisting it in the investigation and prosecution of this matter, and to disclose those materials as necessary to comply with discovery and disclosure obligations in any prosecutions related to this matter.

V. Conclusion

35. Based on the foregoing, I respectfully request that the Court issue the warrant sought herein pursuant to the applicable provisions of the Stored Communications Act, 18 U.S.C. § 2703(b)(1)(A) (for contents) and § 2703(c)(1)(A) (for records and other information), and the relevant provisions of Federal Rule of Criminal Procedure 41.



Special Agent
Federal Bureau of Investigation

Sworn to before me this
1 day of August, 2022


HONORABLE KATHARINE H. PARKER
United States Magistrate Judge
Southern District of New York

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

In the Matter of a Warrant for All
Content and Other Information
Associated with the iCloud Accounts
[REDACTED]@gmail.com and
[REDACTED]@icloud.com
Maintained at Premises Controlled by
Apple Inc., USAO Reference No.
2021R00778

22 MAG 6274

SEARCH WARRANT AND NON-DISCLOSURE ORDER

TO: Apple Inc. ("Provider")

Federal Bureau of Investigation ("Investigative Agency")

1. Warrant. Upon an affidavit of Special Agent [REDACTED] of the Federal Bureau of Investigation, and pursuant to the provisions of the Stored Communications Act, 18 U.S.C. § 2703(b)(1)(A) and § 2703(c)(1)(A), and the relevant provisions of Federal Rule of Criminal Procedure 41, the Court hereby finds there is probable cause to believe the iCloud accounts [REDACTED]@gmail.com and [REDACTED]@icloud.com, maintained at premises controlled by the Provider, contains evidence, fruits, and instrumentalities of crime, all as specified in Attachment A hereto. Accordingly, the Provider is hereby directed to provide to the Investigative Agency, within 30 days of the date of service of this Warrant and Order, the records specified in Section II of Attachment A hereto, for subsequent review by law enforcement personnel as authorized in Section III of Attachment A. The Government is required to serve a copy of this Warrant and Order on the Provider within 14 days of the date of issuance. The Warrant and Order may be served via electronic transmission or any other means through which the Provider is capable of accepting service.

2. Non-Disclosure Order. Pursuant to 18 U.S.C. § 2705(b), the Court finds that there is reason to believe that notification of the existence of this warrant will result in destruction of or tampering with evidence, or otherwise will seriously jeopardize an ongoing investigation. Accordingly, it is hereby ordered that the Provider shall not disclose the existence of this Warrant and Order to the listed subscriber or to any other person for a period of one year from the date of this Order, subject to extension upon application to the Court if necessary, except that Provider may disclose this Warrant and Order to an attorney for Provider for the purpose of receiving legal advice.

3. Sealing. It is further ordered that this Warrant and Order, and the Affidavit upon which it was issued, be filed under seal, except that the Government may without further order of this Court serve the Warrant and Order on the Provider; provide copies of the Affidavit or Warrant and Order as need be to personnel assisting the Government in the investigation and prosecution of this matter; and disclose these materials as necessary to comply with discovery and disclosure obligations in any prosecutions related to this matter.

Dated: New York, New York

8/1/2022
Date Issued

3:14 p.m.
Time Issued

Kathleen H. Park
UNITED STATES MAGISTRATE JUDGE
Southern District of New York

iCloud Search Attachment A

I. Subject Accounts and Execution of Warrant

This warrant is directed to Apple Inc. (the “Provider”), headquartered at 1 Infinite Loop, Cupertino, California 95014, and applies to all content and other information within the Provider’s possession, custody, or control associated with the iCloud accounts [REDACTED]@gmail.com and [REDACTED]@icloud.com (the “Subject Accounts”).

A law enforcement officer will serve this warrant by transmitting it via email or another appropriate manner to the Provider. The Provider is directed to produce to the law enforcement officer an electronic copy of the information specified in Section II below. Upon receipt of the production, law enforcement personnel will review the information for items falling within the categories specified in Section III below.

II. Information to be Produced by the Provider

To the extent within the Provider’s possession, custody, or control, the Provider is directed to produce the following information associated with the Subject Accounts:

a. *Subscriber and payment information.* All subscriber and payment information regarding the Subject Accounts, including but not limited to name, username, address, telephone number, alternate email addresses, registration IP address, account creation date, account status, length of service, types of services utilized, means and source of payment, and payment history.

b. *Device information and settings.* All information about the devices associated with the Subject Accounts, including but not limited to the Integrated Circuit Card ID (“ICCID”) number, the Media Access Control address (“MAC address”), the unique device identifier (“UDID”), the serial number, customer device settings, and repair history.

c. *Transactional records.* All transactional records associated with the Subject Accounts, including any IP logs or other records of session times and durations.

d. *Address book information.* All address book, contact list, or similar information associated with the Subject Accounts.

e. *Call history and voicemails.* All call histories, logs for FaceTime calls, audio voicemails, and visual voicemails associated with the Subject Accounts.

f. *Text message content.* All text messages (including iMessages, Short Message Service (“SMS”) messages, and Multimedia Messaging Service (“MMS”) messages) sent to or from, stored in draft form in, or otherwise associated with the Subject Accounts, including all message content, attachments, and header information (specifically including the source and destination addresses associated with each text message, and the date and time at which each text message was sent).

g. *Email content.* All emails sent to or from, stored in draft form in, or otherwise associated with the Subject Accounts, including all message content, attachments, and header information (specifically including the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email).

h. *Photos and videos.* All photographs or videos associated with the Subject Account, including any photographs or videos found on any iCloud Photo Library, My Photo Stream, or iCloud Photo Sharing service linked to the Subject Accounts. All associated metadata with any photograph or video including the time and date of creation, the author or creator, the means of its creation, and the GPS location information for where a photo or video was taken.

i. *Documents.* All documents stored in or otherwise associated with the Subject Accounts, including all documents in iCloud Drive, and iWork Apps.

j. *Search and web histories.* All search history, web history, bookmarks, and iCloud Tabs.

k. *Third-party application data.* All records, messages, and data relating to third-party applications, including WhatsApp and other third-party messaging applications, stored in or otherwise associated with the Subject Accounts.

l. *Location data.* All location data associated with the Subject Accounts.

m. *iOS Device Backups.* All device backups, and the contents of those backups, including but not limited to messages, web history, and preferences.

III. Review of Information by the Government

Law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review the records produced by the Provider in order to locate any evidence, fruits, and instrumentalities of theft of federal funds and wire fraud, and conspiracy to commit the same, in violation of 18 U.S.C. §§ 371, 666, 1343, and 1349, including the following:

a. Evidence of knowledge or understanding of, or intent to violate, laws and regulations governing the conduct of the 2021 New York City Mayoral campaign on the part of [REDACTED] and its employees, officers, or associates.

b. Evidence relating to coordination between employees, officers, and associates of [REDACTED] and employees, officers, and associates of the 2021 New York City mayoral campaign of Eric Adams (the “Adams Campaign”) concerning political contributions to the Adams Campaign.

c. Evidence relating to payments to employees, officers, and associates of [REDACTED] to facilitate those employees, officers, and associates making political contributions to the Adams Campaign.

d. Evidence relating to coordination or communications between employees, officers, and associates of the Adams Campaign and employees, officers, and associates of the Turkish General Consulate in New York City concerning contributions to the Adams Campaign.

e. Evidence relating to the source of funds for payment or reimbursement of employees, officers, and associates of [REDACTED] for political contributions to the Adams Campaign.

f. Evidence of other individuals or entities who donated to the Adams Campaign before or after receiving transfers of funds similar to the amount of the donation.

g. Identity of any persons or entities involved, wittingly or unwittingly, in straw donations to the Adams Campaign.

h. Passwords or other information needed to access user's online accounts.